局域网中 ARP 攻击与防范

秦 光

(西昌学院 信息技术系,四川 西昌 615013)

【摘 要】分析 ARP 协议的工作原理、ARP 攻击的基本原理与方式,提出预防 ARP 欺骗的常用防范措施。

【关键词】ARP 协议;IP 地址;MAC 地址;ARP 攻击
【中图分类号】TP393.08 【文献标识码】A 【文章编号】1673-1891(2007)02-0064-03

1 引言

ARP 协议[1]是"Address Resolution Protocol"(地址解析协议)的缩写。ARP 协议用来将 IP 地址解析成对应的 MAC 地址,所谓'地址解析'就是主机在发送帧之前将目标 IP 地址转换成目标 MAC 地址的过程。因为局域网的数据传输并不是根据 IP 地址而是按照 MAC 地址进行传输的,所以它是局域网正常通信的基础。由于 ARP 协议缺少必要的身份认证和鉴别机制,安全性十分脆弱,易导致 ARP 欺骗攻击。

近年来,针对网络的攻击不断增加,互联网上也出现了 ARP 欺骗的木马程序或 ARP 攻击软件,如网络执法官、传奇盗号的软件、QQ 盗号的软件、ARP 洪水攻击器 WinArpAttacker 等等,导致密码被盗或造成上网时断时通等现象,已经对局域网构成了严重威胁。

2 ARP 协议及缺陷

2.1 ARP 协议的工作原理

在以太网(Ethernet)中,每一台主机都具有两个地址,一个是 IP 地址,另一个是 MAC 地址。IP 地址是由 32 位二进制数组成,用于在网络层当中标识和查找计算机,它由用户手工分配或者从 DHCP 服务器自动获得;MAC 地址又称为物理地址,由 48 位二进制数组成,用于在数据链路层中标识和查找计算机,它被固化存储在网卡中,并且是全球唯一不可改变的。

两台主机进行直接通信,需要知道目标主机的 IP 地址与 MAC 地址。通过源主机的子网掩码与目标主机的 IP 进行相互操作,可以判断目标主机与源主机是否位于同一网段。将情况分为两种,一种情况是源主机与目标主机在同一网段,如果源主机没有目标主机的 MAC 地址,则以广播的方式发送 ARP 报文,在报文中包含源主机与目标主机的 IP 地址,网段内的所有主机都将收到 ARP 报文,如果网段内某台主机的 IP 与 ARP 报文中的目标主机 IP 一致,就向源主机发送 ARP 回应报文,从而使源主机得到目标主机的 MAC 地址;另一种情况是源主机与目标主机不在同一网段,源主机将 IP 分组发送缺省网关,由网关对分组进行转发,如果源主机没有网关的 MAC 地址,也是通过 ARP 协议来获得。

为了尽量减少网络流量,提高处理的效率。每台主机都保留了一个专用的高速缓存区(cache),即 ARP 缓存,用来存放主机启动以来所有的 IP – MAC 之间的映射记录。当发送信息时,主机首先到高速 cache 的 ARP 表中查找相应的映射关系,若找不到,再利用 ARP 进行地址解析[2]。ARP 缓存表每隔一定时间或者当收到 ARP 应答,都会对 ARP 缓存进行更新,从而保证是最新的地址解析缓存。

2.2 ARP 协议的缺陷[3]

ARP 协议在设计之初没有考虑到网络安全方面的问题,存在设计缺陷,主要表现在两个方面:

(1)任何 ARP 响应都是合法的,ARP 应答不需要认证。ARP 协议中没有规定没有收到查询不能发送应答包,因此任何主机在没有 ARP 请求的时候可

收稿日期:07 – 01 – 08
作者简介:秦光(973 –),男,讲师,硕士,主要从事计算机专业课程的教学研究与网络管理工作。

以做出应答，许多系统会接爱 ARP 的响应，并对 ARP 缓存进行更新。

(2)ARP 协议没有提供检测 IP – MAC 缓存的真实性的机制，也不用维护其有效性和一致性。可能出现多个 IP 地址到一个 MAC 地址的映射，也可以出现某 IP 到一个不存在的 MAC 地址的映射情况出现。

由于 ARP 设计的缺陷，导致出现了 ARP 欺骗攻击的情况发生,由此可能导致安全隐患。

3 ARP 欺骗攻击

3.1 ARP 攻击的基本原理

ARP 的攻击有多种形式，但攻击的基本原理是类似的。下面通过一个例子来讲述 ARP 攻击的基本原理。

假设一网络由一个 HUB 和 3 台 PC (A、B、C)构成,其中

A 的地址为 IP：172. 16. 0. 1，MAC：11 – 11 – 11 – 11 – 11 – 11

B 的地址为 IP：172. 16. 0. 2，MAC：22 – 22 – 22 – 22 – 22 – 22

C 的地址为 IP：172. 16. 0. 3，MAC：33 – 33 – 33 – 33 – 33 – 33

主机 A 与主机 C 进行正常通信时,先查看主机 A 的 ARP 缓存：

C: > arp – a

Interface: 172. 16. 0. 1 —— 0x3

Internet Address　　Physical Address　　Type

172. 16. 0. 3　　33 – 33 – 33 – 33 – 33 – 33　　dynamic

B 向 A 发送一个仿造的 ARP 应答,数据为发送方 IP 地址 17216. 0. 3 (C 的 IP 地址)，MAC 是 44 – 44 – 44 – 44 – 44 – 44 (伪造的 MAC)，当 A 接收到 B 伪造的应答，就会更新 A 的 ARP 缓存，现在主机 A 的 ARP 缓存更新了,再次查看：

C: > arp – a

Interface: 172. 16. 0. 1 —— 0x3

Internet Address　　Physical Address　　Type

172. 16. 0. 3　　44 – 44 – 44 – 44 – 44 – 44　　dynamic

由于局域网的数据传输不是按 IP 而是按 MAC 进行的，现在 172. 16. 0. 3 的 MAC 地址在主机 A 的缓存中被改为不存在的 MAC 地址,从而造成主机 A 与主机 C 无法正常通信。

3.2 ARP 的攻击方式

(1)简单的欺骗攻击

通过发送伪造的 ARP 包来欺骗路由和目标主机,让目标主机认为这是一个合法的主机,便完成了欺骗。这种欺骗多发生在同一网段内,因为路由不会把本网段的数据包向外转发，当然实现不同网段的攻击也有方法，便要通过 ICMP 协议来告诉路由器重新选择路由。

(2)交换环境的嗅探[4]

现在的网络多是交换环境，网络内数据的传输被锁定特定目标。既已确定的目标通信主机，在 ARP 欺骗的基础之上，可以把自己的主机伪造成一个中间转发站来监听两台主机之间的通信。前面的例子将 HUB 换成交换机，如果主机 A 与主机 C 正常通信，主机 B 可以通过 ARP 欺骗，从而实现转发主机 A 与主机 C 通信的数据包，达到在交换网络下主机 B 对主机 A 与主机 C 通信数据的嗅探。

(3)MAC Flooding

局域网中楼层交换机多采用二层交换机，自身维护一个 ARP 缓存，用于映射 MAC – PORT (MAC 地址与端口)的对应关系,由于缓存可容纳的映射条目数有限，如果发送大量 MAC 地址不重复的 ARP 数据包，产生溢出交换机的 ARP 表，造成交换机的 DOS (拒绝服务),不能正常运转,这是一个比较危险的攻击,使得整个交换机所连接的网络瘫痪。

4 ARP 攻击的防范

ARP 攻击具有一定突发性与隐蔽性，由于 ARP 协议是低层协议，所以常见的防火墙与杀病毒软件无法进行拦截,很难防范。根据 ARP 攻击特点是利用主机对 ARP 应答的无条件信任,篡改主机的 ARP 缓存，从而达到攻击目的，因此需要保证主机 ARP 缓存表中的 IP – MAC 地址映射关系的正确,阻止非法篡改 ARP 缓冲从而避免主机受到攻击。常用的防范措施有：

(1)IP + MAC 访问控制

单纯依靠 IP 或 MAC 来建立信任关系是不安全的,理想的安全关系建立在 IP + MAC 的基础上。

(2)ARP 高速缓存超时设置

在 ARP 高速缓存中的表项一般都要设置超时

值,缩短这个超时值可以防止ARP表的溢出。

(3)主动查询

在某个正常的时刻,做一个IP和MAC对应的数据库,以后定期检查当前的IP和MAC对应关系是否正常,定期检测交换机的流量列表,查看丢包率。

(4)设置静态ARP缓存表

每台主机都有一个临时存放IP-MAC的对应表,ARP攻击就通过更改这个缓存来达到欺骗的目的,使用静态的ARP来绑定正确的MAC是一个有效的方法。找出网关正确的MAC,然后通过ARP-S IP MAC来建立用静态表。此时"TYPE"项变成了"static",静态类型这个状态下是不会再接受到ARP包而改变本地缓存,从而有效的防止ARP攻击。缺点是静态的ARP条目在每次重启后都要消失而需要重新设置。

(5)利用防ARP攻击软件

由于ARP攻击对同一网段内的计算机影响较大,为了不受网段的ARP攻击影响而无法上网,可以采用防止ARP攻击的软件,如ANTIARP、arpFix等,这类软件帮助计算机正确记录下本网段的网关MAC地址,从而防止网段内的ARP欺骗。

5 结束语

ARP协议由于存在缺陷,导致局域网易受到ARP欺骗攻击,出现用户上网时断时续等现象,对局域网具有较大的破坏性。弄清ARP攻击的原理与攻击方式后,只要采取相应防范措施,可以避免遭受ARP攻击。

参考文献:

[1] Network Working Group David C. Plummer. Request For Comments: 826 (DCP@ MIT-MC). [OL]. November 1982, http://www.cnpaf.net/Class/Rfcen/0532918533864384.html.

[2]徐敬东,张建忠. 计算机网络[M]. 北京:清华大学出版社,2002: 95-96.

[3]马军,王岩. ARP协议攻击及其解决方案[J]. 微计算机信息,2006,22(5):70-71.

[4] Dieter Gollmann. 计算机安全[M]. 北京:人民邮电出版社,2003: 191-192.

ARP Attack and Guard in the Local Area Network

QIN Guang

(Department of Information Technology, Xichang College, Xichang, Sichuan 615013)

Abstract: This paper analyzes the ARP protocol, the ARP attack theory and the method, and proposes prevents the ARP cheat the commonly used guard measure.

Key words: ARP protocol; IP address; MAC address; ARP attack

(责任编辑:张荣萍)